Domain 1:
Security and Risk Management

CISSP Domain 1 Security & Risk Management Detailed Notes

Code:	CISSPD1SRMN
Version:	2
Date of version:	1/12/2018
Created by:	AL Nafi Content Writer
Approved by:	Nafi Content reviewers
Confidentiality level:	For members only

Change history

Date	Version	Created by	Description of change
1/12/2018	1	Nafi Edu Dept	AL Nafi mentors created the first set of notes.
2/5/2019	2	Nafi Edu Dept	AL Nafi mentors created the first set of notes.

Table of contents

1. Purpose, scope and users

The purpose of this document is to define CISSP domain for Nafi members Only. Please be honest to yourself and with Al Nafi and do not share this with anyone else. Everyone can join Al Nafi as we are so economical to begin with.

These notes covers all the key areas of Domain 1 and the notes are good until a new revision of CISSP syllabus comes from ISC2. Normally the cycle is around 3 years so since we had our last revision in 2018 June, the next update to the CISSP syllabus is expected around June 2021.

Please follow the following 5 step program if you want to master CISSP domain and pass the exam inshAllah.

1. Watch all the CISSP videos on the portal 8-10 times. Soak yourself with Brother Faisal words in what he is teaching and try to ask questions. Think like a Security Manager who does everything with due care and due diligence.
2. Read all the presentations slides and the detailed notes at least 8-10 times. Pay attention to additional reading material recommended by Brother Faisal during his videos.
3. Practice all the flash cards multiple times on our website.
4. Practice all the MCQ's on our website. (Those who score 85% in 10 out of 15 tests [The last 10 sets are counted towards exam payment by Al Nafi] Al Nafi will pay their exam fee inshAllah. Please give dawah to 50 people to join al nafi if they want to study inshAllah)
5. Go for the CISSP exam once you are approved by Al Nafi and your examination fee is paid.

2. Understand and apply concepts of (CIA) confidentiality, integrity and availability

2.1. CIA Triad explanation:

As a security professional or a trainee you need to know CIA (Confidentiality, integrity and availability) down to its core.

We will focus on the three key principles as we will now refer them as CIA triad. In the field of information security, we have assets which can be tangible (something you can touch) for example your organization computers, servers, employees, data etc. and non-tangible (something you cannot touch) for example your reputation, your market share, your share or stock value etc. all of these assets requires security and the first thing as a security practitioner you will do is to utilize the CIA principle to assess what level of security you need to apply as per your business, security and compliance requirements. This is true even for data that is stored in any form, be it electronically or in printed hardcopy. It also applies to any systems, mechanisms, techniques used to process/manipulate/store/transmits that data.

For CIA examples please review the presentation notes and video files.

Throughout the course the CIA triad will be used extensively so please brush up your concepts as they relate to Confidentiality, integrity and availability.

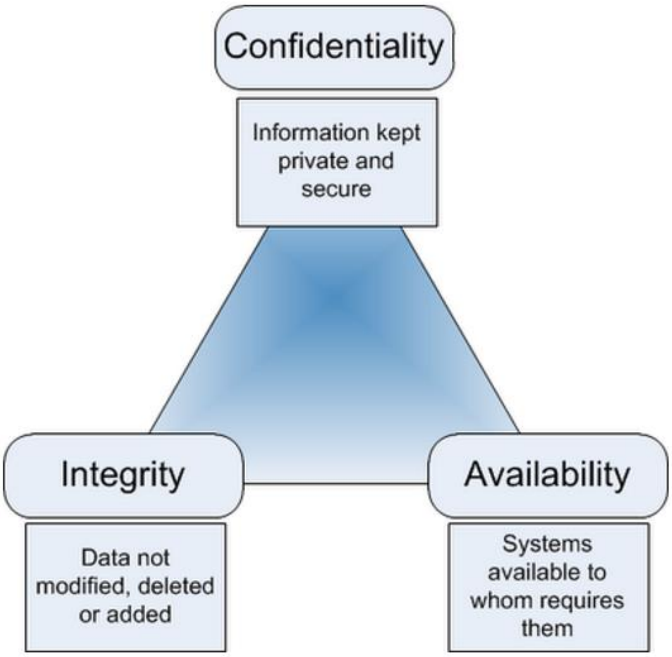
The CIA Connection

The CIA connection:
CIA means Confidentiality, Integrity, Availability

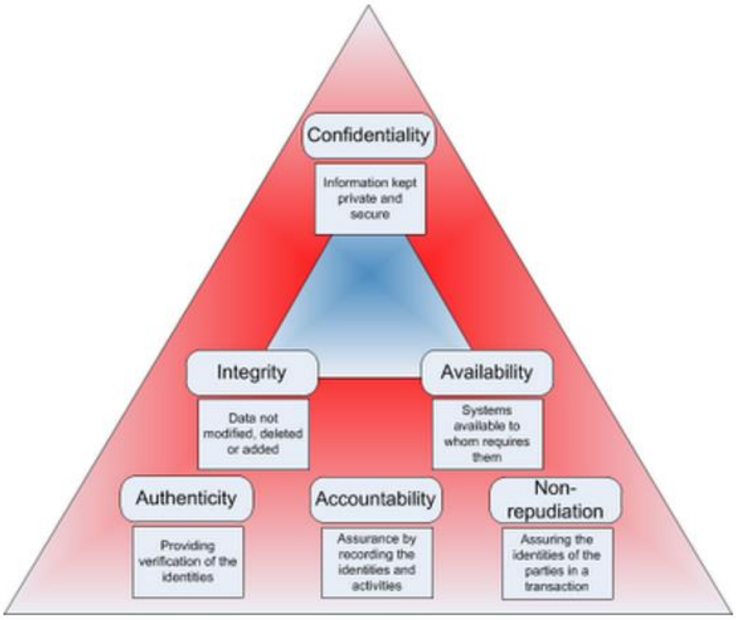
Confidentiality:
Only those who are authorizes to have access to the data can access the data.

Integrity:
Only those who are authorizes to make changes can modify the data

Availability:
Only those who are authorizes to access data can do so when permitted.


Confidentiality
Information kept private and secure
Integrity
Data not modified, deleted or added
Availability
Systems available to whom requires them

Reference http://geraintw.blogspot.com/2012/09/cia-infosec.html


Confidentiality
Information kept private and secure
Integrity
Data not modified, deleted or added
Availability
Systems available to whom requires them
Authenticity
Providing verification of the identities
Accountability
Assurance by recording the identities and activities
Non-repudiation
Assuring the identities of the parties in a transaction

Reference http://geraintw.blogspot.com/2012/09/cia-infosec.html

3. Evaluate and apply security governance principles

3.1. Executive management

Person or group of people who have delegated responsibility from the governing body for implementation of strategies and policies to accomplish the purpose of the organization.

NOTE 1 Executive management form part of top management: For clarity of roles, these notes distinguishes between two groups within top management: the governing body and executive management.

NOTE 2 Executive management can include Chief Executive Officers (CEOs), Heads of Government Organizations, Chief Financial Officers (CFOs), Chief Operating Officers (COOs), Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and like roles.

3.2. Governing body

Person or group of people who are accountable for the performance and conformance/compliance of the organization

NOTE governing body forms part of top management: For clarity of roles, this standard distinguishes between two groups within top management: the governing body and executive management.

3.3. Governance of information security

System by which an organization’s information security activities are directed and controlled

3.4. Stakeholder

Any person or organization that can affect, be affected by, or perceive themselves to be affected by an activity of the organization.

NOTE a decision maker can be a stakeholder.

4. Security Governance definition

Security Governance describes the principles and processes that, together, form the governance of information security. Governance principles of information security are accepted rules for governance action or conduct that act as a guide for the implementation of governance. A governance process for information security describes a series of tasks enabling the governance of information security and their interrelationships. It also shows a relationship between governance and the management of information security.

Meeting the needs of stakeholders and delivering value to each of them is integral to the success of information security in the long term. To achieve the governance objective of aligning information security closely with the goals of the business and to deliver value to stakeholders, this sub-clause sets out six action-oriented principles.

The principles provide a good foundation for the implementation of governance processes for information security. The statement of each principle refers to what should happen, but does not prescribe how, when or by whom the principles would be implemented because these aspects are dependent on the nature of the organization implementing the principles. The governing body should require that these principles be applied and appoint someone with responsibility, accountability, and authority to implement them.

4.1. Principle 1: Establish organization-wide information security

Governance of information security should ensure that information security activities are comprehensive and integrated. Information security should be handled at an organizational level with decision-making taking into account business, information security, and all other relevant aspects. Activities concerning physical and logical security should be closely coordinated.

To establish organization-wide security, responsibility and accountability for information security should be established across the full span of an organization’s activities. This regularly extends beyond the generally perceived ‘borders’ of the organization e.g. with information being stored or transferred by external parties.

4.2. Principle 2: Adopt a risk-based approach

Governance of information security should be based on risk-based decisions. Determining how much security is acceptable should be based upon the risk appetite of an organization, including loss of competitive advantage, compliance and liability risks, operational disruptions, reputational harm, and financial loss.

To adopt an information risk management appropriate to the organization, it should be consistent and integrated with the organization’s overall risk management approach. Acceptable levels of information security should be defined based upon the risk appetite of an organization, including the loss of competitive advantage, compliance and liability risks, operational disruptions, reputational harm, and financial losses. Appropriate resources to implement information risk management should be allocated by the governing body.

4.3. Principle 3: Set the direction of investment decisions

Governance of information security should establish an information security investment strategy based on business outcomes achieved, resulting in harmonization between business and information security requirements, ,both in short and long term,, thereby meeting the current and evolving needs of stakeholders.

To optimize information security investments to support organizational objectives, the governing body should ensure that information security is integrated with existing organization processes for capital and operational expenditure, for legal and regulatory compliance, and for risk reporting.

4.4. Principle 4: Ensure conformance with internal and external requirements

Governance of information security should ensure that information security policies and practices conform to relevant mandatory legislation and regulations, as well as committed business or contractual requirements and other external or internal requirements.

To address conformance and compliance issues, the governing body should obtain assurance that information security activities are satisfactorily meeting internal and external requirements by commissioning independent security audits.

4.5. Principle 5: Foster a security-positive environment

Governance of information security should be built upon human behaviour, including the evolving needs of all the stakeholders, since human behaviour is one of the fundamental elements to support the appropriate level of information security. If not adequately coordinated, the objectives, roles, responsibilities and resources may conflict with each other, resulting in the failure to meet business objectives. Therefore, harmonization and concerted orientation between the various stakeholders is very important.

To establish a positive information security culture, the governing body should require, promote and support coordination of stakeholder activities to achieve a coherent direction for information security. This will support the delivery of security education, training and awareness programs.

4.6. Principle 6: Review performance in relation to business outcomes

Governance of information security should ensure that the approach taken to protect information is fit for purpose in supporting the organization, providing agreed levels of information security. Security performance should be maintained at levels required to meet current and future business requirements.

To review performance of information security from a governance perspective, the governing body should evaluate the performance of information security related to its business impact, not just effectiveness and efficiency of security controls. This can be done by performing mandated reviews of a performance measurement program for monitoring, audit, and improvement, and thereby link information security performance to business performance.

5. Aligning the security function to the organization business strategy, goals, mission and objectives

Organization security program MUST always be aligned closely to overall purpose, business strategy, objectives, goals and missions. Even in this day and age, security is still treated as an afterthought. In case of Pakistan at least security is still treated as an expense rather than a business enabler. However in case of organizations who are developing, providing and or support security products it's a different case. It is absolute imperative that organizations have a robust security strategy and program which is aligned tightly to organization business strategy, goals, mission and objectives. In todays connected world, no organization can survive without a robust security strategy and plan in place.

There you as a security practitioner must understand the organization functions, its strategy from operational and IT perspectives, to better create and or enhance a security function. Security function that does not align with proper organizational goals can lead to issues which can result in decisions that can severely impact organizations capability to run and or expand its business. It will also inhibit its productivity, create undue costs and hinder strategic intent.

6. Organizational Processes and their impact to security

Security governance is a process which defines how a decision is made within an organization. This task is accomplished in different ways as per organization culture, management style and other variety of factors.

Inn large organizations the task is much more organized and at times can be more complicated as there are multiple levels of decision makers which are required to be involved. IN small private business and or organizations the decision making process may be as simple as one or two person, who at the end of the day make a decision based on consultation or derived from a personal experience of the decision makers.

In government or public organizations there is a chartered legislative body or a corporation which makes strategic decision based defined policies, procedures, board of directors etc.

Each organization will have its own process for making decision, based on a defined structure, goals, nature of the industry, regulations.

Some companies/organizations create a governance committee, which is a formal body of personnel who recommends and or decisions. Governance committees are mostly required for most non-profit organizations as well. The governance committee recruits and selects board members and determines if the board as a whole and or an individual member(s) are perform in an optimum fashion.

7. Added definitions

7.1. Acquisition

If any organization decides to purchase a business unit or a whole organization. If the organization decides to purchase another business unit to have as a subsidiary, the security implications are extensive. If there is a significant difference in security policies and practices between the entities, the security professionals in both groups will have to decide how best to align the two, with guidance and final decision from senior management.

7.2. Merger

Much like an acquisition, a merger of two organizations entails aligning the security governance of the resulting entity.

7.3. Divestiture

If an organization decides to sell off or cede control of a subsidiary, a considerable amount of effort will have to go into determining which of the resulting entities controls proprietary property, to include data, which may entail a great deal of effort on the part of the security personnel. In each of these examples, external entities, such as regulators and investors, may have additional input and control in determining the outcome. These examples are not exhaustive; many organizational decisions will have vast security ramifications.

8. Organizational Roles and Responsibilities

An organization’s hierarchy is often determined by the goals of the organization or which industry it operates in. This structure can have a bearing on how security governance is created and implemented, or even how security functions are performed.

The following are a sampling of various roles pertaining to security encountered in many organizations. This list is in no way inclusive of all types of organizational structures and is not presented as a definitive guide to these roles; it is simply a way to demonstrate the form of some organizations and the bearing of some roles on organizational security.

8.1. Senior Management

The upper strata of the organization, comprising those officers and executives that have the authority to obligate the organization and to dictate policy. These can include such roles as president, vice president, chief executive officer (CEO), chief operating officer (COO), chief information officer (CIO), chief security officer (CSO), chief financial officer (CFO), and the like. Usually, these roles include personnel with some direct legal or financial responsibilities according to statute or regulation. Senior management is typically responsible for mandating policy, determining the strategic goals for the organization, and making final determinations according to the organizational governance for both security and non-security topics.

8.2. Security manager/security officer/security director

Often, this is the senior security person within an organization. In some cases, the organization has a CSO (mentioned in the preceding entry of this list), in which case the security officer is a member of senior management. When the senior security role is not a member of senior management, the reporting hierarchy is an essential element of determining the importance and influence security has within the organization. For instance, an organization wherein the security manager reports directly to the CEO places a great deal of importance on security; an organization that has the security manager reporting to an administrative director, who in turn reports to a vice president, who reports to senior management, obviously does not. The security manager is typically responsible for advising senior management on security matters, may assist in drafting security policy, manages day-to-day security operations, represents the organization's security needs in groups and meetings such as the Configuration Management Board and similar committees, contracts for and selects security products and solutions, and may manage the organization's response to incidents and disasters.

Note: According to industry best practices, the security manager should not report to the same role/department that is in charge of information technology (IT) because the functions are somewhat adversarial (the security team will be reporting on/reviewing the operations and productivity of the IT team). Having the same department responsible for both functions would constitute a form of conflict of interest. The exception to this is when both the security office and the IT department report to the chief information officer (CIO); this is usually an acceptable form of hierarchy.

8.3. Security personnel

The security practitioners within the organization. These can include administrators, analysts, incident responders, and so forth. This group may also include personnel from disciplines other than IT security, such as physical security and personnel security. Security personnel are tasked with performing the security processes and activities within the organization. Security personnel usually report to the security manager/director/officer.

8.4. Administrators/technicians

IT personnel who regularly perform work within the environment may have security duties as well. These can include secure configuration of systems, applying secure networking, reporting potential incidents, and so forth. Positions in this category include but are not limited to: system administrators (often Tech Support and Help Desk personnel) and network administrators/engineers. This group typically reports to the IT director or CIO.

8.5. Users

Employees, contractors, and other personnel who operate within the IT environment on a regular basis. While this role does not have specific security duties per se, users are required to operate the systems in a secure fashion, and they are usually required to sign a formal agreement to comply with security guidance. Users may also be co-opted and trained to report potential security incidents, acting as a rudimentary form of intrusion detection. Users typically report to their functional managers.

9. Security Control Frameworks

In formalizing its security governance, an organization might implement a security control framework; this is a notional construct outlining the organization's approach to security, including a list of specific security processes, procedures, and solutions used by the organization. The framework is often used by the organization to describe its security efforts, for both internal tracking purposes and for demonstration to external entities such as regulators and auditors. There are a variety of security frameworks currently popular in the industry, each offering benefits and capabilities, usually designed for a certain industry, type of organization, or approach to security. The following list of framework examples is by no means exhaustive or intended to be exclusive; the security practitioner should have a working familiarity with the frameworks on this list, as well as whatever framework is used by their own organization (if any). Some of these frameworks will be discussed in more detail later in the course.

9.1. ISO 27001/27002

The International Standards Organization (ISO) is recognized globally, and it is probably the most pervasive and used source of security standards outside the United States (American organizations often use standards from other sources).

ISO 27001 is known as the information security management system (ISMS) and is a comprehensive, holistic view of security governance within an organization, mostly focused on policy. ISO 27002 is a comprehensive list of security controls that can be applied to an organization; the organization uses ISO 27002 to select the controls appropriate to its own ISMS, which the organization designs according to ISO 27001. ISO standards are notably thorough, well-recognized in the industry, and expensive relative to other standards. Use of ISO standards can allow an organization to seek and acquire specific standards-based certification from authorized auditors.

9.2. COBIT

Created and maintained by ISACA, the COBIT framework (currently COBIT 5) is designed as a way to manage and document enterprise IT and IT security functions for an organization. COBIT widely uses a governance and process perspective for resource management and is intended to address IT performance, security operations, risk management, and regulatory compliance.

9.3. ITIL

An IT service delivery set of best practices managed by Axelos, a joint venture between the British government and a private firm. ITIL (formerly the Information Technology Infrastructure Library, now simply the proper name of the framework) concentrates on how an organization's IT environment should enhance and benefit its business goals. ITIL is also mapped to the ISO 20000 standard, perhaps the only non-ISO standard to have this distinction. This framework also offers the possibility for certification, for organizations that find certification useful.

9.4. RMF

NIST, the U.S. National Institute of Standards and Technology, publishes two methods that work in concert (similar to how ISO 27001 and 27002 function); the Risk Management Framework (RMF), and the applicable list of security and privacy controls that goes along with it (respectively, these documents are Special Publications (SPs) 800-37 and 800-53). While the NIST SP series is only required to be followed by federal agencies in the United States, it can easily be applied to any kind of organization as the methods and concepts are universal. Also, like all American government documents, it is in the public domain; private organizations do not have to pay to adopt and use this framework. However, there is no private certification for the NIST framework.

9.5. CSA STAR

The Cloud Security Alliance (CSA) is a volunteer organization with participant members from both public and private sectors, concentrating—as the name suggests—on security aspects of cloud computing. The CSA publishes standards and tools for industry and practitioners, at no charge. The CSA also hosts the Security, Trust, and Assurance Registry (STAR), which is a voluntary list of all cloud service providers who comply with the STAR program framework and agree to publish documentation on the STAR website attesting to compliance. Customers and potential customers can review and consider cloud vendors at no cost by accessing the STAR website. The STAR framework is a composite of various standards, regulations, and statutory requirements from around the world, covering a variety of subjects related to IT and data security; entities that choose to subscribe to the STAR program are required to complete and publish a questionnaire (the Consensus Assessments Initiative Questionnaire (CAIQ), colloquially pronounced “cake”) published by CSA. The STAR program has three tiers, 1–3, in ascending order of complexity. Tier 1 only requires the vendor self-assessment, using the CAIQ. Tier 2 is an assessment of the organization by an external auditor certified by CSA to perform CAIQ audits. Tier 3 is in draft form as of the time of publication of this CBK; it will require continuous monitoring of the target organization by independent, certified entities.

9.6. Due Care/Due Diligence

Due care is a legal concept pertaining to the duty owed by a provider to a customer. In essence, a vendor has to engage in a reasonable manner so as not to endanger the customer: the vendor’s products/services should deliver what the customer expects, without putting the customer at risk of undue harm. An example to clarify the concept: if a customer buys a car from the vendor, the vendor should have designed and constructed the car in a way so that the car can be operated in a normal, expected manner without some defect harming the customer. If the user is driving the car normally on a road and a wheel falls off, the vendor may be culpable for any resulting injuries or damage if the loss of the wheel is found to be the result of insufficient care on the part of the vendor (if, say, the wheel mount was poorly designed, or the bolts holding the wheel were made from a material of insufficient strength, or the workers assembling the car did so in a careless or negligent way). This duty is only required for reasonable situations; if, for instance, the customer purposefully drove the car into a body of water, the vendor does not owe the customer any assurance that the car would protect the customer, or even that the car would function properly in that circumstance.

NOTE: There is a joke regarding the standard of reasonableness that lawyers use—"Who is a reasonable person? The court. The court is a reasonable person." Meaning that the "standard" is actually quite ambiguous and arbitrary: the outcome of a case hinging on a determination of "reasonable" action is wholly dependent on a specific judge on a specific day, and judges are only people with opinions. Due diligence, then, is any activity used to demonstrate or provide due care. Using the previous example, the car vendor might engage in due diligence activities such as quality control testing (sampling cars that come off the production line for construction/assembly defects), subjecting itself to external safety audit, prototype and regular safety testing of its vehicles to include crash testing, using only licensed and trained engineers to design their products, and so forth. All of these actions, and documentation of these actions, can be used to demonstrate that the vendor provided due care by performing due diligence. In the IT and IT security arena, due diligence can also take the form of reviewing vendors and suppliers for adequate provision of security measures; for instance, before an organization uses an offsite storage vendor, the organization should review the vendor's security governance, and perhaps even perform a security audit of the vendor to ensure that the security provided by the vendor is at least equivalent to the security the organization itself provides to its own customers. Another form of due diligence for security purposes could be proper review of personnel before granting them access to the organization's data, or even before hiring; this might include background checks and personnel assurance activities. (Personnel security measures, which provide a measure of due diligence, will be discussed in more detail later in this domain.)

NOTE: In recent years, regulators and courts (both of which are often tasked with determining sufficient provision of due care) have found certain activities to be insufficient for the purpose of ensuring due diligence, even though those activities were previously sufficient. Specifically, publishing a policy is an insufficient form of due diligence; to meet the legal duty, an organization must also have a documented monitoring and enforcement capability in place and active to ensure the organization is adhering to the policy.

10.Information technology — Security techniques — Information security risk management

10.1. Scope of ISO 27005 which is used for Security Risk Management

This International Standard provides guidelines for information security risk management. This International Standard supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this International Standard. This International Standard is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

11.Terms and definitions for Security Risk Management

11.1. What does consequence means?

- Outcome of an event
- An event can lead to a range of consequences.
- A consequence can be certain or uncertain and in the context of information security is usually negative.
- Consequences can be expressed qualitatively or quantitatively.
- Initial consequences can escalate through knock-on effects.

11.2. What does control means

- Measure that is modifying risk
- Controls for information security include any process, policy, procedure, guideline, practice or organizational structure, which can be administrative, technical, management, or legal in nature which modify information security risk.
- Controls may not always exert the intended or assumed modifying effect.
- Control is also used as a synonym for safeguard or countermeasure.

11.3. What does event means?

- Occurrence or change of a particular set of circumstances
- An event can be one or more occurrences, and can have several causes.
- An event can consist of something not happening.
- An event can sometimes be referred to as an “incident” or “accident”.

11.4. What does external context means?

- External environment in which the organization seeks to achieve its objectives
  External context can include:
- the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- Key drivers and trends having impact on the objectives of the organization; and
- Relationships with, and perceptions and values of, external stakeholders.

11.5. What does internal context means?

- Internal environment in which the organization seeks to achieve its objectives

Internal context can include:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- information systems, information flows and decision-making processes (both formal and informal);
- relationships with, and perceptions and values of, internal stakeholders;
  - – the organization's culture;
  - – standards, guidelines and models adopted by the organization; and
  - – form and extent of contractual relationships.

11.6. What does level of risk means?

- Magnitude of a risk expressed in terms of the combination of consequences and their likelihood

11.7. Likelihood

- Chance of something happening
- In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).
- The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

11.8. Residual risk

- risk remaining after risk treatment
- Residual risk can contain unidentified risk.
- Residual risk can also be known as “retained risk”.

11.9. Risk

- Effect of uncertainty on objectives
- An effect is a deviation from the expected — positive and/or negative.
- Objectives can have different aspects (such as financial, health and safety, information security, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
- Risk is often characterized by reference to potential events and consequences, or a combination of these.
- Information security risk is often expressed in terms of a combination of the consequences of an information security event and the associated likelihood of occurrence.
- Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.
- Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

11.10. Risk analysis

- Process to comprehend the nature of risk and to determine the level of risk
- Risk analysis provides the basis for risk evaluation and decisions about risk treatment.
- Risk analysis includes risk estimation.

11.11. Risk assessment

- Overall process of risk identification risk analysis and risk evaluation

11.12. Risk communication and consultation

- Continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk
- The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of risk.
- Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:
    - a process which impacts on a decision through influence rather than power; and
    - an input to decision making, not joint decision making.

11.13. Risk criteria

- terms of reference against which the significance of a risk is evaluated
- Risk criteria are based on organizational objectives, and external and internal context.

- Risk criteria can be derived from standards, laws, policies and other requirements.

11.14. Risk evaluation

- Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
- Risk evaluation assists in the decision about risk treatment.

11.15. Risk identification

- Process of finding, recognizing and describing risks
- Risk identification involves the identification of risk sources, events, their causes and their potential consequences.
- Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.

11.16. Risk management

- Coordinated activities to direct and control an organization with regard to risk
- This International Standard uses the term 'process' to describe risk management overall. The elements within the risk management process are termed 'activities'

11.17. Risk treatment

Process to modify risk

Risk treatment can involve:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk with another party or parties (including contracts and risk financing); and
- retaining the risk by informed choice.

- Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".
- Risk treatment can create new risks or modify existing risks.

11.18. Stakeholder

- Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
- A decision maker can be a stakeholder.

12.Risk Management Approach as per ISO 27005 Standard

This is the main standard that all Nafi members must read 10 times to ensure that they can draw the figure below from memory inshAllah.

A systematic approach to information security risk management is necessary to identify organizational needs regarding information security requirements and to create an effective information security management system (ISMS). We will learn ISMS implementation in our ISO 27001 AL Nafi course. This approach should be suitable for the organization´s environment, and in particular should be aligned with overall enterprise risk management. Security efforts should address risks in an effective and timely manner where and when they are needed. Information security risk management should be an integral part of all information security management activities and should be applied both to the implementation and the ongoing operation of an ISMS.

Information security risk management should be a continual process. The process should establish the external and internal context, assess the risks and treat the risks using a risk treatment plan to implement the recommendations and decisions. Risk management analyses what can happen and what the possible consequences can be, before deciding what should be done and when, to reduce the risk to an acceptable level.

Information security risk management should contribute to the following:

- Risks being identified
- Risks being assessed in terms of their consequences to the business and the likelihood of their occurrence
- The likelihood and consequences of these risks being communicated and understood
- Priority order for risk treatment being established
- Priority for actions to reduce risks occurring
- Stakeholders being involved when risk management decisions are made and kept informed of the risk management status
- Effectiveness of risk treatment monitoring
- Risks and the risk management process being monitored and reviewed regularly
- Information being captured to improve the risk management approach
- Managers and staff being educated about the risks and the actions taken to mitigate them
- The information security risk management process can be applied to the organization as a whole, any discrete part of the organization (e.g. a department, a physical location, a service), any information system, existing or planned or particular aspects of control (e.g. business continuity planning).

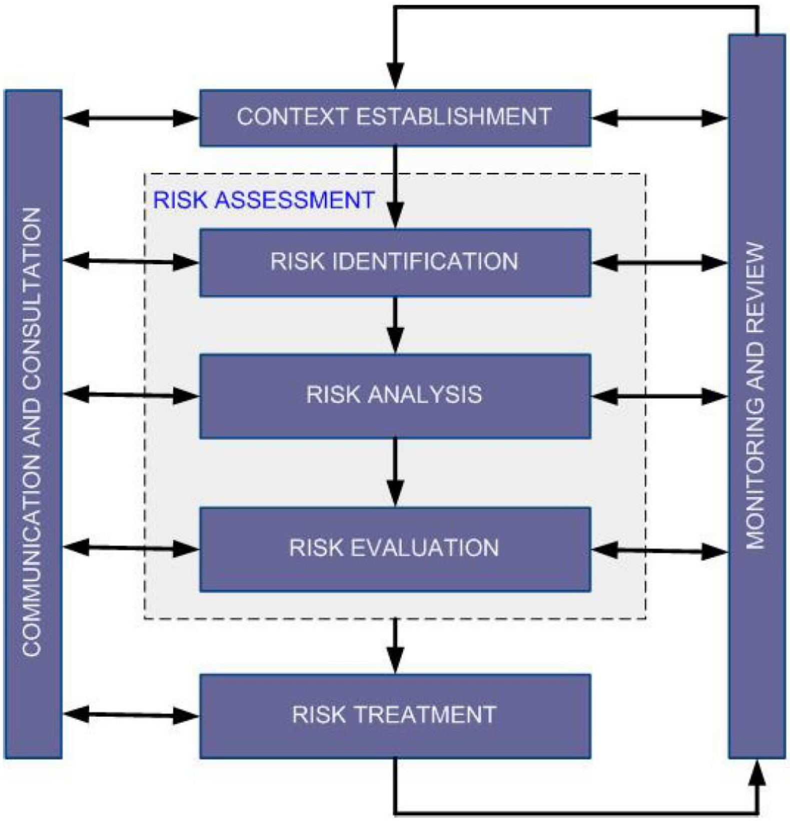


Figure 1

The next figure 2 shows how RISK Management process works in a detailed fashion. The information security risk management process consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation, and risk monitoring and review.

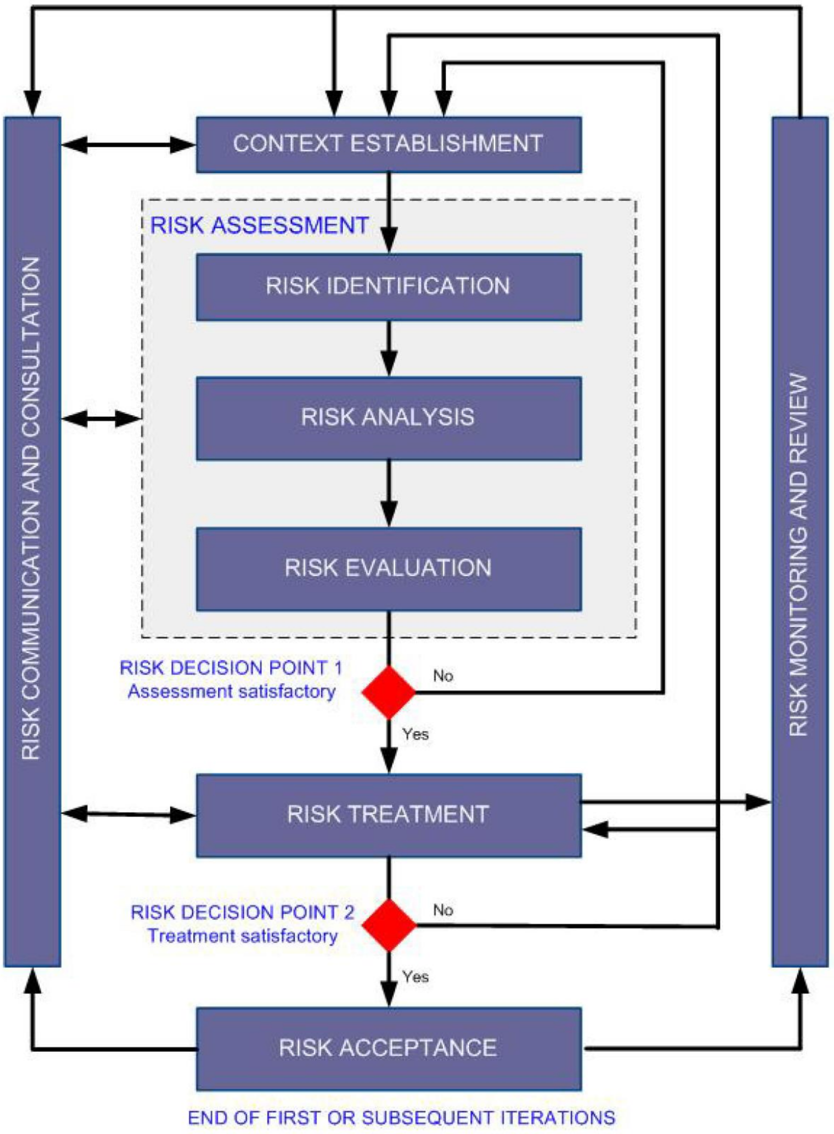


Figure 2 — Illustration of an information security risk management process

As Figure 2 illustrates, the information security risk management process can be iterative for risk assessment and/or risk treatment activities. An iterative approach to conducting risk assessment can increase depth and detail of the assessment at each iteration. The iterative approach provides a good balance between minimizing the time and effort spent in identifying controls, while still ensuring that high risks are appropriately assessed.

The context is established first. Then a risk assessment is conducted. If this provides sufficient information to effectively determine the actions required to modify the risks to an acceptable level then the task is complete and the risk treatment follows. If the information is insufficient, another iteration of the risk assessment with revised context (e.g. risk evaluation criteria, risk acceptance criteria or impact criteria) will be conducted, possibly on limited parts of the total scope. The effectiveness of the risk treatment depends on the results of the risk assessment.

Note that risk treatment involves a cyclical process of:

- assessing a risk treatment;
- deciding whether residual risk levels are acceptable;
- generating a new risk treatment if risk levels are not acceptable; and
- assessing the effectiveness of that treatment

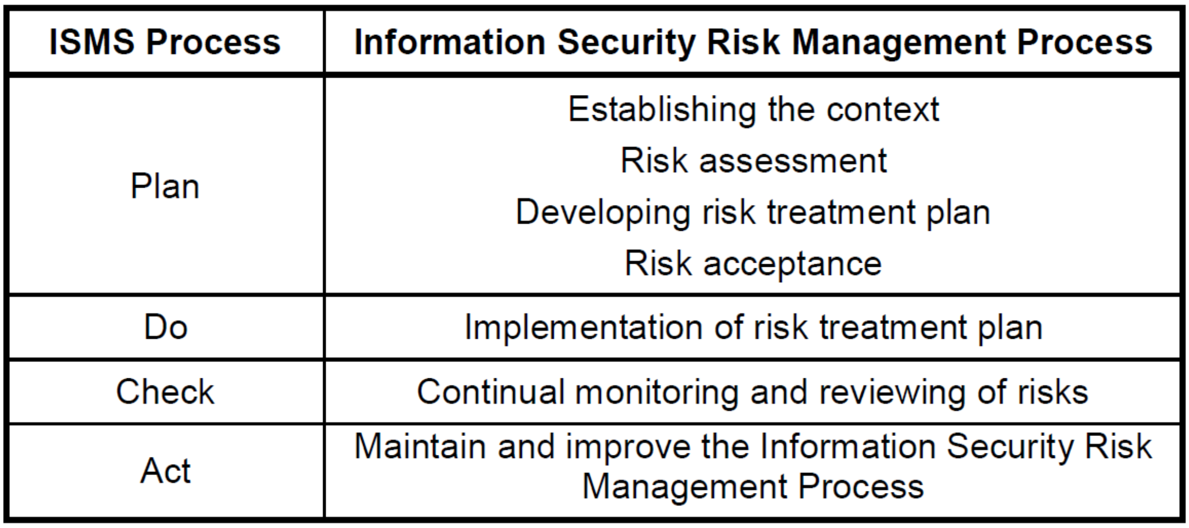
It is possible that the risk treatment will not immediately lead to an acceptable level of residual risk. In this situation, another iteration of the risk assessment with changed context parameters (e.g. risk assessment, risk acceptance or impact criteria), if necessary, may be required, followed by further risk treatment (see Figure 2, Risk Decision Point 2) above.

The risk acceptance activity has to ensure residual risks are explicitly accepted by the managers of the organization. This is especially important in a situation where the implementation of controls is omitted or postponed, e.g. due to cost. During the whole information security risk management process it is important that risks and their treatment are communicated to the appropriate managers and operational staff. Even before the treatment of the risks, information about identified risks can be very valuable to manage incidents and may help to reduce potential damage. Awareness by managers and staff of the risks, the nature of the controls in place to mitigate the risks and the areas of concern to the organization assist in dealing with incidents and unexpected events in the most effective manner. The detailed results of every activity of the information security risk management process and from the two risk decision points should be documented.

ISO/IEC 27001 specifies that the controls implemented within the scope, boundaries and context of the ISMS need to be risk based. The application of an information security risk management process can satisfy this requirement. There are many approaches by which the process can be successfully implemented in an organization. The organization should use whatever approach best suits their circumstances for each specific application of the process.

In an ISMS, establishing the context, risk assessment, developing risk treatment plan and risk acceptance are all part of the “plan” phase. In the “do” phase of the ISMS, the actions and controls required to reduce the risk to an acceptable level are implemented according to the risk treatment plan. In the “check” phase of the ISMS, managers will determine the need for revisions of the risk assessment and risk treatment in the light of incidents and changes in circumstances. In the”act” phase, any actions required, including additional application of the information security risk management process, are performed.

The following table summarizes the information security risk management activities relevant to the four phases of the ISMS process:



ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Developing risk treatment plan Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

Figure 3 Alignment of ISMS and Information Security Risk Management Process

13.Security Controls

Security controls are methods, tools, mechanisms, and processes used in risk mitigation. Security controls can function in two general ways: as safeguards, which reduce risk impact/likelihood before the realization of the risk has occurred, and countermeasures, which reduce the impact/likelihood afterwards. For example, a wall could be a safeguard, preventing hostile people from entering the facility, while a motion sensor could be considered a countermeasure as it sends an alert when someone has entered the area in an unauthorized fashion. Security controls should be chosen according to a cost/benefit analysis, comparing the expense of acquiring, deploying, and maintaining the control against the control's ability to reduce the impact/likelihood of a specific risk (or set of risks). It is also crucial to weigh the operational impact that will be caused by the control itself against the benefit of continuing that business function with the risk reduction offered by that control.
As Dr. Eugene "Spaf" Spafford of Purdue University once put it: "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then, I have my doubts." http://spaf.cerias.purdue.edu/quotes.html

14.Traditional Model

One traditional method for selecting the appropriate security controls has been the use of the "loss expectancy" model: annual loss expectancy (ALE) = single loss expectancy (SLE) x annual rate of occurrence (ARO)

In detail, it works like this: The SLE is the expected negative impact related to a particular risk (the risk being assessed). Most often, this is expressed monetarily. It is calculated by determining the value of the asset that might be affected (or lost) and multiplying it by an "exposure factor"—a percentage that represents the amount of damage resulting from that type of loss.

So: SLE = asset value (AV) x exposure factor (EF) The ARO is the number of times per year a given impact is expected, expressed as a number. So, the ALE is the SLE multiplied by the ARO, which gives us the estimated annual cost related to a particular risk. The value of the ALE to the organization is that it allows the organization to determine whether the cost of a particular kind of control for a specific risk is worth the investment.

15.Applicable Types of Controls

Security controls can be arranged according to many criteria. One way to consider controls is by the way the controls are implemented.

15.1. Technical/logical controls:

Controls implemented with or by automated or electronic systems. Examples include firewalls, electronic badge readers, access control lists, and so on. Many IT systems include some kind of technical control capacity or functionality; for instance, routers can be set to reject traffic that may be indicative of possible attacks.

15.2. Physical controls:

Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, and so forth. In modern organizations, many physical control systems are linked to technical/ logical systems, such as badge readers connected to door locks.

15.3. Administrative controls:

Controls implemented through policy and procedure. Examples include access control processes and requiring multiple personnel to conduct a specific operation. Administrative controls in modern environments are often enforced in conjunction with physical and/or technical controls, such as an access-granting policy for new users that requires login and approval by the hiring manager.

16.Security Control Categories

Another way to group security controls is by how they take effect. In the security industry, controls are typically arranged into these categories:

16.1. Directive:

Controls that impose mandates or requirements. These can include policies, standards, signage, or notification, and are often combined with training.

16.2. Deterrent:

Controls that reduce the likelihood someone will choose to perform a certain activity. These can include notification, signage, cameras, and the noticeable presence of other controls.

16.3. Preventative:

Controls that prohibit a certain activity. These can include walls and fences; they prohibit people from entering an area in an unauthorized manner.

16.4. Compensating:

Controls that mitigate the effects or risks of the loss of primary controls. Examples include physical locks that still function if an electronic access control system loses power, or personnel trained to use fire extinguishers/hoses in the event a sprinkler system does not activate.

16.5. Detective:

Controls that recognize hostile or anomalous activity. These can include motion sensors, guards, dogs, and intrusion detection systems.

16.6. Corrective:

Controls that react to a situation in order to perform remediation or restoration. Examples include fire suppression systems, intrusion prevention systems, and incident response teams.

16.7. Recovery:

Controls designed to restore operations to a known good condition following a security incident. These can include backups and disaster recovery plans.

This form of categorization is not absolute or distinct; many controls can fall into several categories, depending on their implementation and operation. For instance, surveillance cameras can control that are deterrent (just the presence of cameras discourages someone from entering a surveyed area, for fear of being observed), detective (when combined with live monitoring by guards or a motion-sensing capability), and compensating (when providing additional detection capability that augments gate guards or other controls). Controls of the various types (administrative, technical, and physical) can be used in each of the categories.

When selecting and implementing security controls, it is always preferable to use multiple types and implement them among the various categories than to rely on one type or category; this is called defense in depth (also known as layered defense), where controls of various types and kinds overlap each other in coverage. There are two reasons to implement defense in depth:

1. Relying on a single control type or category increases the possibility that a single control failure could lead to enhanced risk. For instance, if the organization were to rely solely on technical controls and power was interrupted, those controls would not function properly. Moreover, a new vulnerability might be discovered in a specific control; if that was the sole control your organization relied on, your organization would become completely exposed.

2. Using multiple types and categories of controls forces the aggressor to prepare multiple means of attack instead of just one. By making the task of the attacker more complicated, we reduce the number of possible attackers (many people know one thing well, but few people know many things well). For instance, combining strong technical and physical controls could require the aggressor to have both hacking and physical intrusion toolkits, which increases the price of the attack for attacker, thereby reducing the number of potential attackers.

17.Monitoring and Measurement

Implementation of security controls is not the final action necessary for risk mitigation; the security professional must monitor the function and operation of security controls for the organization to determine if they are performing correctly and that they continue to provide the risk coverage as intended. Often referred to as a security control assessment (SCA) a plan and process for determining the proper function and management of controls is necessary and should be customized to the needs of the organization.

This is very similar to an audit with specific focus on security controls and includes performance of those controls. The security team is often tasked with assembling SCA data and presenting a report to senior management, detailing which controls are not performing as expected and which risks are not being addressed by the current control set. This information might be gathered by the security team itself through the use of automated monitoring tools, or it might be delivered by internal sources (such as the IT department) as part of a self-reporting mechanism, or from external sources (such as a third-party security monitoring vendor).

The security practitioner must collect all relevant data and distill it into a form that is understandable and useful to management. This security control monitoring effort should not be a singular event or even a recurring task; the industry standard for security control maintenance and improvement is a continual, ongoing, enduring activity. Threats continue to evolve, the organization's IT environment is continually being updated and modified, and security tools continue to improve; these situations require constant action on the part of security practitioners. Other control assessment techniques include vulnerability assessments and penetration tests:

1. Vulnerability assessment: Often performed with automated tools, the vulnerability assessment reviews the organization's IT environment for known vulnerabilities, cataloging and often sending alerts for any detections. NOTE: vulnerability assessments are often limited in the respect that they only detect known vulnerabilities; relying wholly on vulnerability assessments to determine the organization's risk profile is inadequate, because there may exist vulnerabilities that have not yet been discovered and are not in the signature database of the assessment tool.

2. Penetration test: A trusted party (internal or external to the organization) tries to gain access to the organization's protected environment to simulate an external attack and test the organization's security defenses. There are many ways to structure a penetration test, including requiring that the adversarial parties (the organization's security team and the penetration testers) have no knowledge beyond what an attacker would have: the security team is not given forewarning that the test is taking place, and the testers are not given details about the organization's environment or security. Ethical penetration testing requires that any test not create a risk to health and human safety or destroy property. It is essential to properly coordinate any penetration test before the engagement to stipulate any limitations on the scope or nature of the test.

Risk Management frameworks that will be covered in a separate course will be during the implementation ISO 27001, ISO 31000, along with ISACA Risk IT and NIST publications. Please wait for that course to come online during our 2019 classes soon inshAllah.

18.Understand and Apply Threat Modeling Concepts and Methodologies

As explained in the presentations, a threat is something that might cause a threat to be realized. To anticipate and counter anthropomorphic threats, the security industry uses a technique called threat modeling, which entails looking at an environment, system, or application from an attacker's viewpoint and trying to determine vulnerabilities the attacker would exploit. The end state of this process is addressing each of the vulnerabilities discovered during threat modeling to ensure an actual attacker cannot use them.

In many threat modeling techniques, an abstract, nontechnical abstraction of the target (whether it is an organization or an IT system/ application) is necessary before reviewing the details of the target itself. Workflow diagrams (also referred to as dataflow diagrams or flowcharts) are frequently used for the purpose; the threat modeling team creates a conceptual view of how the target actually functions—how data and processes operate in the target from start to finish. This allows the threat modeling team to understand where an attacker might affect the target, by understanding potential locations (in time, space, and the process) of vulnerabilities.

In some threat models used for specific targets (systems/applications, instead of the overall organization), another element is used (mostly in addition to, not in lieu of, the abstract); incorporating those same threat modeling techniques into the detailed specifics of the target. With this technique, designers can identify and troubleshoot potential vulnerabilities during the development and acquisition of the target instead of waiting until the target reaches the production environment.

This practice (securing a system/application) during development is less expensive and time-consuming than addressing issues after the item has entered production. The candidate should certainly be familiar with one particular threat modeling tool: STRIDE. STRIDE, created by Microsoft, is actually a threat classification system used to inform software developers during the development process. These are the elements of STRIDE:

Spoofing identity: the type of threat wherein an attacker poses an entity other than the attacker, often as an authorized user.

Tampering with data: when the attacker attempts to modify the target data in an unauthorized way.

Repudiation: when the attacker, as a participant of a transaction, can deny (or conceal) the attacker's participation in that transaction.

Information disclosure: just like it sounds, this category can include both inadvertent release of data (where an authorized user discloses protected data accidentally to unauthorized users, or gains access to material that their authorization should not allow) and malicious access to data (an attacker getting unauthorized access).

Denial of service (DoS): an attack on the availability aspect of the CIA triad; creating a situation in the target where authorized users cannot get access to the system/ application/data.

Elevation of privilege: when an attacker not only gains access to the target but can attain a level of control with which to completely disable/destroy the entire target system.

19.Minimum Security Requirements

To provide appropriate levels of security, a fundamental understanding of the desired outcomes is necessary. Security professionals achieve this by gathering a set of minimum security requirements to use as a goal. This minimum set of requirements should be created for every level granularity in an operation: the organization as a whole (where the minimum security requirements become the level of acceptable risk), the overall IT environment, each network that is included in the environment, each system in each network, and even each component. Moreover, this practice (gathering minimum security requirements) should not be limited only to IT and data activity, but it should also be included in project management and process functions.

Some hints for effectively gathering minimum security requirements:

- Involve stakeholders in the development/acquisition/ planning process as soon as possible (close to the start of the endeavor).
- Ensure that requirements are specific, realistic, and measurable.
- Record and document all elements of the discussion and outcome.
- When soliciting input from the customer, restate your understanding of their requests back to them to confirm what they intended to say and what you comprehend.
- Don't choose tools or solutions until the requirements are understood; too often in our field, we already have a preferred technology in mind when starting a project, when we should instead only select a specific product once we fully comprehend the objectives. Otherwise, we tend to allow the technology to drive business functions, instead of the other way around.
- If possible, create diagrams, models, and prototypes to solidify mutual understanding of the requirements before commencing full-scale development and production.

20.Service Level Requirements

When an organization uses an external provider for managed services (for example, a cloud service, or a contractor that maintains the organization's data center), the parties must establish a mutual understanding of exactly what will be provided, under which terms, and at what times. This should include a detailed description of both performance and security functions. As with other projects, the organization has to establish a set of minimum requirements for this effort to be successful; in this type of case, however, the organization is not usually able to dictate requirements unilaterally and must instead cooperate with the provider. Together, the parties will construct a business contract explicitly stating the terms of the arrangement. One part of this contract should be the service level agreement (SLA), which defines the minimum requirements and codifies their provision. Every element of the SLA should include a discrete, objective, numeric metric with which to judge success or failure, otherwise, the SLA implementation will not be fair or reasonable for either party.

21.Contractual, Legal, Industry Standards, and Regulatory Requirements

Every organization operates under some type of external mandate. This mandate can come in the form of simple contracts, as part of the organization's interactions with suppliers and customers; the organization is compelled to fulfill their contractual obligations. Mandates can also come in the form of governmental imposition; governments create regulations, either through legislative or administrative means, and organizations must adhere to the regulations relevant to the industry and manner in which the organization operates. There are also traditional and cultural mandates, arising in every society; some of these take the form of standards, which each organization is held to by custom and, in some jurisdictions, by legal precedent and liability.

Compliance is adherence to a mandate, regardless of the source. Almost every modern organization is required to demonstrate compliance to the various mandates the organization is subject to. Compliance is used in our industry as a term that means both the action on the part of the organization to fulfill the mandate and the tools, processes, and documentation that demonstrate adherence. Many modern mandates address a specific need: personal privacy. Privacy is the right of a human being to control the manner and extent to which information about him or her is distributed.

Privacy mandates take all forms: contractual, regulatory, and customary. Organizations are often reviewed to determine compliance with applicable mandates. Often, the tools, processes, and activities used to perform compliance reviews are referred to as audits (or auditing).

22.Contractual Mandates

A contract is an agreement between parties requiring them to perform in some way and the terms for performance. Contracts are an instrumental tool in business where the contract obligates the organization; contracts are either used or implicit in every business transaction. Contracts could be as simple as the exchange of money for a product, or a complicated, long-term arrangement requiring hundreds of pages of contract documentation.

An organization enters into a contract voluntarily, and law and custom dictate that every party to a contract will fulfill the requirements of the contract unless they are unable to do so. The importance of contracts has been codified in most countries as law, to the extent that any party not fulfilling their contractual obligations may be forced to do so (or pay recompense) if the other party/parties to the contract seek relief from the courts.

In many cases, parties to a contract may have the right to review the progress and activity of each other to ensure the terms of the contract are being met (this is also stipulated in the contract). This may involve inspection of raw data, a measure of some performance, or audits; these actions may be performed by the parties to the contract or by external third parties on their behalf.

It is important that all Nafi members who are following Cyber security, Offensive security, IT Audit, IT Governance and IT Risk management tracks should attend the following courses offered by AL Nafi:

- ISO 27001 Lead Implementation
- ISO 27017 Lead Implementation
- ISO 27018 Lead Implementation
- ISO 20000 Lead Implementation
- ISO 22301 Lead Implementation
- PCI DSS QSA Training
- GDPR Training

23.Legal Standards

Legal standards are set by courts in decisions that set precedent; that is, the judgments a court has made previously become the standard of acceptable practice for future behavior. This precedent informs other courts in making determinations, for instance, of reasonable expectations for parties to a contract—the due care mentioned earlier in this domain. Organizations use these standards in the formulation of their own strategy and governance as a means of setting acceptable risk. When a court makes a decision about due care, organizations that will be subject to similar circumstances make plans according to that standard out of recognition of liability they might face for noncompliance.

24.Common Privacy Law Tenets

Many privacy laws address similar concepts associated with individual personal data, that have become common globally. The candidate should be familiar with these general concepts:

- Notification: The data subject (the individual human related to the personal data in question) should be notified before any of their personal data is collected or created.
- Participation: The subject should have the option not to take part in the transaction, if the subject chooses not to share their personal data.
- Scope: Any personal data collected or created should be for a specific purpose; this purpose should be legal and ethical and be included in the notification aspect of the transaction, as well as inform the limitation aspect.
- Limitation: Any personal data should only be used for the purpose identified in the scope aspect of the transaction; any additional use would require repeating the notification and participation aspects.

- Accuracy: Any personal data should be factual and current; data subjects should have a means to correct/edit any information about the subject in a simple, timely manner.
- Retention: Personal data should not be kept any longer than is necessary for the purpose, or as required by applicable law.
- Security: Any entity that has possession of personal data is responsible for protecting it.
- Dissemination: Any entity that has possession of personal data should not share it with any other entity, nor release it, without the express permission of the data subject and in accordance with applicable law.

25.Cyber Crimes and Data Breaches

The modern IT landscape affords criminals with a host of options for engaging in nefarious activity, including updated versions of traditional crimes. Criminals may, for instance, conduct age-old activities such as fraud, theft, blackmail, and extortion but use modern appliances to extend their reach, speed, and efficiency. There are also new criminal statutes that have created new classes of crimes the security practitioner should be aware of.

A brief description of some (but certainly not all) possible computer related crimes:

- **Malware:** In many jurisdictions, governments have made the creation and dissemination of malicious software a crime.
- **Unauthorized access**: The modern version of trespassing, the simple act of accessing a system/network in an unauthorized manner is against the law in many countries.
- **Ransomware:** A new version of the old crime of extortion; the attacker gains access (often illegally) to the victim's data, encrypts it, and offers to sell the victim the encryption keys to recover the data. Ransomware tools have become so pervasive and effective that, in many cases, even federal law enforcement entities have advised victims to pay the ransom
- **Theft:** Stealing data—or hardware on which data resides—can be a lucrative criminal enterprise.
- **Illegal use of resources**: In many situations, attackers conduct unauthorized access not to get anything directly from the victim but to use the victim's IT assets for the attacker's benefit. This can take the form of storage (where the attacker is using the victim's memory to stash files and data the attacker has acquired elsewhere), or processing (where the attacker is using the victim's CPU to conduct malicious activity such as staging DDoS attacks).
- **Fraud**: By engaging the victim in some way (often through an appeal to the victim's greed or sympathy), the attacker is able to illegally acquire the victim's money. Common tactics include: the attacker posing as someone else (often as someone related to the victim, through social media); the attacker gaining access to the victim's bank account; the attacker preying on those who are not media-savvy such as the elderly.
- **Data breach** notification is another area of law that has become ubiquitous; many countries (and jurisdictions within countries, such as U.S. states) have created legislation requiring any entity that has personal data within its possession to notify the subjects of that data if the data is disclosed in any unauthorized fashion. Any organization that is not in compliance with these laws (that is, any organization that loses personal data and does not make sufficient notification in a timely manner) faces severe financial penalties in many jurisdictions. The security practitioner should be aware of all such applicable laws for every jurisdiction in which their organization operates.

26.Import/Export Controls

The security practitioner should be aware that IT hardware and software is often subject to international trade restrictions, mainly for national defense purposes. In particular, encryption tools are seen by many governments as a threat to global stability and rule of law. One such restriction scheme is the Wassenaar Agreement, a multilateral export control restriction program involving 41 participating countries; these countries agree not to distribute (export) certain technologies (including both weapons and, of more concern to our field, cryptographic tools) to regions where an accumulation of these materials might disturb the local balance of power between nation-states. Security practitioners employed or operating in either a Wassenaar signatory country or in a region where import of these materials is controlled by the Agreement need to be aware of these prohibitions and understand what encryption tools may or may not be used. Many countries have their own internal laws governing the import/export of encryption technologies in addition to international treaties. For instance, Russia and some Baltic States, Myanmar, Brunei, and Mongolia have outright bans on the import of cryptographic

27.Privacy Terms

Many data privacy laws use a common terminology; the candidate should be familiar with the following terms and concepts.

- Personally identifiable information (PII): PII, as it is referred to in the industry, is any data about a human being that could be used to identify that person. The specific elements of what data constitutes PII differs from jurisdiction to jurisdiction and from law to law. These are some elements that are considered PII in some jurisdictions and laws:

    - Name
    - Tax identification number/Social Security number
    - Home address
    - Mobile telephone number
    - Specific computer data (MAC address, IP address of the user’s machine)
    - Credit card number
    - Bank account number
    - Facial photograph

  Under some laws, PII is referred to by other terms as was mentioned earlier in this domain: for instance, medical data in the United States is referred to as electronic protected health information (ePHI) under HIPAA.

- **Data subject**: The individual human being that the PII refers to.

- **Data owner/data controller**: An entity that collects or creates PII. The data owner/controller is legally responsible for the protection of the PII in their control and liable for any unauthorized release of PII. Ostensibly, the owner/controller is an organization; the legal entity that legitimately owns the data. In some cases (in certain jurisdictions, under certain laws), the data owner is a named individual, such as an officer of the company, who is the nominal data owner. In actual practice, however, we usually think of the data owner as the managerial person or office that has the most day-today use and control of the data; that is, the department or branch that created/collected the data and which puts the data into use for the organization.

- **Data processor:** Any entity, working on behalf or at the behest of the data controller, that processes PII. Under most PII-related laws, “processing” can include absolutely anything that can be done with data: creating, storing, sending, computing, compiling, copying, destroying, and so forth. While the data processor does have to comply with applicable PII law, it is the data owner/controller that remains legally liable for any unauthorized disclosure of PII even if the processor is proven to be negligent/malicious.

- **Data custodian:** The person/role within the organization who usually manages the data on a day-to-day basis on behalf of the data owner/controller. This is often a database manager or administrator; other roles that might be considered data custodians could be system administrators or anyone with privileged access to the system or data set.

28.Policy

The written aspect of governance (including security governance) is known as policy. Policies are documents published and promulgated by senior management dictating and describing the organization’s strategic goals (“strategic” entails long-term, overarching planning that addresses the whole of the organization; it is possible to have goals that are not strategic to the organization, such as goals for a specific department, project, or duration). Security policies are those policies that address the organization’s security goals and might include such areas as data classification, access management, and so on.

Typically, policies are drafted by subject matter experts, shared among stakeholders for review and comment, revised, then presented to senior management for final approval and publication. This is especially true for security policy, which is often a topic of which senior management has little understanding and insight, and it relies greatly on security practitioners for advice and guidance.

29.Standards

Standards are specific mandates explicitly stating expectations of performance or conformance. Standards can either come from within the organization (internal) or from external sources such as statutory or administrative law, case law (court decisions that set precedent), professional organizations, and/or industry groups. Some standards are detailed and specific; an example might be an industry standard for configuring a certain IT component or device. Some standards are general and describe a goal, outcome, or process; an example might be a law that sets a standard declaring, “the data controller is required to use physical access control measures to prevent unauthorized removal of hardware containing PII.”

Organizations are required to comply with standards to which they subscribe or which are applicable to the organization; failure to do so can result in prosecution or fines assessed by law enforcement/regulators or can increase and enhance the organization’s liability.

An example, for demonstration purposes: a retail company has some PII related to its customers, including their contact information and shopping habits. In the wake of a data breach, investigators determine that the company was storing data in files that could be accessed with default administrative usernames and passwords, which is directly contrary to all current industry standards and common security practice. Because not conforming to the standard demonstrates a form of negligence, in addition to the costs of resolving the breach, the company may face additional expenses in the form of lawsuits from customers whose data was exposed and fines from regulators who oversee the protection of personal information. If the company had taken good faith steps to protect the data in a professional manner (including adherence to best practices and industry standards), the company would still incur expenses related to resolving the loss but would have attenuated the liability from the additional costs.

30.Procedures

Procedures are explicit, repeatable activities to accomplish a specific task. Procedures can address one-time or infrequent actions (such as a disaster recovery checklist) or common, regular occurrences (for instance, daily review of intrusion detection logs). Like standards, procedures aid the organization by demonstrating due diligence and avoiding liability. Proper documentation of procedures (in both creating the procedures and in executing them) and training personnel how to locate and perform procedures is necessary for the organization to derive benefit of procedures.

31.Guidelines

- Guidelines are similar to standards in that they describe practices and expectations of activity to best accomplish tasks and attain goals. However, unlike standards, guidelines are not mandates but rather recommendations and suggestions. Guidelines may be created internally, for use by the organization, or come from external sources such as industry participants, vendors, and interested parties. There is a general hierarchy of importance typically associated with these governance elements; while not applicable in all cases, usually:

- Policy is at the pinnacle of the hierarchy; the organization's policy is informed by applicable law(s) and specifies which standards and guidelines the organization will follow. Senior management dictates policy, so all activity within the organization should conform to policy.

- Standards are next; the organization's policies should specify which standards the organization adheres to, and the organization can be held accountable for not complying with applicable standards.

- Guidelines inform the organization how to conduct activities; while not mandatory, they can be used to shape and inform policies and procedures, and how to accomplish compliance with standards.

- Procedures are the least powerful of the hierarchy, but they are the most detailed; processes describe the actual actions personnel in the organization will take to accomplish their tasks. Even though they may be considered the bottom of the hierarchy, they are still crucial and can be used for obviating liability and demonstrating due diligence.

32.Business Continuity Requirements

A detailed breakdown of Business continuity planning (BCP) and disaster recovery planning (DRP) will be shared during the ISO 22301 training to ensure that this domain is thoroughly covered from examination perspective. However the below notes will provide you all a good foundation inshAllah.

There is always a risk that the organization will experience a drastic and dramatic event that threatens the existence of the organization itself; these events can take the form of natural disaster, civil unrest, international war, and other major situations. The security practitioner is often called on to address this type of risk and to plan accordingly.

The actions, processes, and tools for ensuring an organization can continue critical operations during a contingency are referred to as business continuity (BC). "Critical operations" (sometimes referred to as "critical path" or "mission critical functions") are those activities and functions that the organization needs to perform to stay operational; they are a subset of the overall operation of the organization. For instance, during contingency operations, an organization might suspend janitorial functions or hiring procedures but might continue sales and financial activity (depending on the essential needs of the organization).

Disaster recovery (DR) efforts are those tasks and activities required to bring an organization back from contingency operations and reinstate regular operations. Typically, these functions act in concert; the same personnel, assets, and (generally) activities will be used to conduct business continuity and disaster recovery efforts; they are often referred to in conjunction with the term "business continuity and disaster recovery" (BCDR).

32.1. Develop and Document Scope and Plan

To properly provide the correct assets for dealing with contingency situations, the organization must determine several essential elements first:

- What is the critical path?
- How long can the organization survive an interruption of that critical path?
- How much data can the organization lose and still remain viable?
- We will discuss the critical path determinations in the next section of this module. Here, we'll address the other two elements.

- The maximum allowable downtime (MAD) (also referred to as the maximum tolerable downtime (MTD)) is the measure of how long an organization can survive an interruption of critical functions; if the MAD is exceeded, the organization will no longer be a viable unit.

32.2. Recovery time objective (RTO)

The recovery time objective (RTO) is the target time set for recovering from any interruption—the RTO must necessarily be less than the MAD.

Senior management must set the RTO, based on their expert knowledge of the needs of the organization, and all BCDR strategy and plans must support achieving the RTO.

NOTE: The term “recovery” in the context of the RTO is not a return to normal operations, but it is instead a goal for recovering availability of the critical path. This is a temporary state that the organization will endure until it is feasible to return to regular status.

32.3. Recovery Point Objective (RPO)

The recovery point objective (RPO) is a measure of how much data the organization can lose before the organization is no longer viable. The RPO is usually measured not in storage amounts (gigabytes/terabytes/petabytes) but instead in units of time: minutes, hours, days, depending on the nature of the organization. Senior management will also set the RPO that will be used along with the RTO to inform BCDR plans.

32.4. Business Impact Analysis (BIA)

The BIA is the effort to determine the value of each asset belonging to the organization, as well as the potential risk of losing assets, the threats likely to affect the organization, and the potential for common threats to be realized. This is a management process that may or may not involve the security office. However, the BIA will also be an instrumental tool for the security function as it is usually the security office that is required to craft and execute the BCDR plan and tasks. Along with determining the value of other assets, the BIA will also reveal the critical path of the organization; without knowing the critical path, it is impossible to properly plan BCDR efforts.

There are many ways to conduct a BIA and make asset value determinations. The following is a partial list of methods that might be used, their benefits, and potential challenges:

S**urvey**: Interview asset owners/data controllers to determine their assessment of the value of the organization’s property they oversee. This method allows for the people closest to the assets to offer input but is also subject to inherent bias.

Financial audit: Review the acquisition/purchase documentation to aggregate value data for all assets in the organization. This offers a thorough review of assets but is prone to variance in actual value because value changes over time (increasing or decreasing, depending on the type of asset and its purpose/use).

Customer response: Surveys of customers can aid the organization in determining which aspects of the operation are most valuable to creating goodwill and long-term revenue. However, customers only see a limited portion of the overall operations and can’t know the source of the value chain.

There are accounting and auditing firms that perform holistic organizational valuation as their business, often as preparation for the sale/acquisition of the organization by another entity. These consultants have expertise and knowledge of this process that may offer an advantage over performing the tasks internally.

The BIA should also consider externalities, such as likely threats and the potential for those threats to manifest. Depending on the nature of the organization’s work, the senior management may want to consider investing in business intelligence services; these are external consultants that constantly glean information from threat sources (hacktivist and terror organizations, open source news reporting, government and industry information feeds, malware management firms, and so on) and customize reports for their clients. The organization may also want to consider creating its own threat intelligence unit, depending on the size and scope of both the organization and its potential attackers.